JP 3278721 B abstract

1/3,AB/1

DIALOG(R)File 351:Derwent WPI
(c) 2003 Thomson Derwent. All rts. reserv.

008953086
WPI Acc No: 1992-080355/199210
XRPX Acc No: N92-060198

Secure time stamping method for digital documents - transmits document to stamping authority to add time data to form receipt and applies cryptographic signature before returning to author

Patent Assignee: HABER S A (HABE-I); STORNETTA W S (STOR-I); BELL COMMUNICATIONS RES INC (BELL-N); BELL COMMUNICATIONS RES (BELL-N); BELL COMMUNIC RES I (BELL-N); TELCORDIA TECHNOLOGIES INC (TELC-N)
Inventor: HABER S A; STORNETTA W S; STORNETTA W

Number of Countries: 017 Number of Patents: 014
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9203000	A	19920220				199210 B
US 5136646	A	19920804	US 91666896	A	19910308	199234
US 5136647	A	19920804	US 90561888	A	19900802	199234
EP 541727	A1	19930519	EP 91917680	A	19910730	199320
			WO 91US5386	A	19910730	
JP 6501571	W	19940217	JP 91516026	A	19910730	199412
			WO 91US5386	A	19910730	
US 34954	E	19950530	US 90561888	A	19900802	199527
			US 93156120	A	19931122	
EP 541727	A4	19951025	EP 91917680	A		199620
CA 2088371	C	19980811	CA 2088371	A	19910730	199843
EP 541727	B1	19991117	EP 91917680	A	19910730	199953
			WO 91US5386	A	19910730	
DE 69131789	E	19991223	DE 631789	A	19910730	200006
			EP 91917680	A	19910730	
			WO 91US5386	A	19910730	
ES 2142307	T3	20000416	EP 91917680	A	19910730	200026
JP 3278721	B2	20020430	JP 91516026	A	19910730	200230
			WO 91US5386	A	19910730	
JP 3281881	B2	20020513	JP 91516026	A	19910730	200234
			JP 2001204357	A	19910730	
JP 2002092220	A	20020329	JP 91516026	A	19910730	200238
			JP 2001204357	A	19910730	

Priority Applications (No Type Date): US 91666896 A 19910308; US 90561888 A 19900802; US 93156120 A 19931122
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9203000	A		34		
Designated States (National): CA JP					
Designated States (Regional): AT BE CH DE DK ES FR GB GR IT LU NL SE					
US 5136646	A		8	H04L-009/00	
US 5136647	A		10	H04L-009/00	
EP 541727	A1	E	34	H04L-009/00	Based on patent WO 9203000
Designated States (Regional): BE CH DE ES FR GB IT LI NL SE					
JP 6501571	W		34	G09C-001/00	Based on patent WO 9203000
US 34954	E		10	H04L-009/00	Reissue of patent US 5136647
CA 2088371	C			H04L-009/00	

EP 541727	B1 E		H04L-009/00	Based on patent WO 9203000
Designated States (Regional): BE CH DE ES FR GB IT LI NL SE				
DE 69131789	E		H04L-009/00	Based on patent EP 541727
				Based on patent WO 9203000
ES 2142307	T3		H04L-009/00	Based on patent EP 541727
JP 3278721	B2	14	G09C-001/00	Previous Publ. patent JP 6501571
				Based on patent WO 9203000
JP 3281881	B2	14	G09C-001/00	Div ex application JP 91516026
				Previous Publ. patent JP 2002092220
JP 2002092220	A	13	G06F-017/60	Div ex application JP 91516026

Abstract (Basic): WO 9203000 A

A digital representation of the document is transmitted from an originator to an outside agency. The outside agency creates a receipt comprising a digital representation of then current time, and at least a portion of a digital representation of the document. The receipt is certified at the outside agency by means of a varifiable digital cryptographic signature scheme. The temporal sequence of digital documents in a series is also clarified.

ADVANTAGE - Reliable method of document verification for e.g. intellectual property uses.

Dwg.1/5

Abstract (Equivalent): US 5136646 A

The system protects the secrecy of the document text and provides a tamper-proof time seal establishing an author's claim to the temporal existence of the document. Initially, the document may be condensed to a single number by means of a one-way hash function, thus fixing a unique representation of the document text. The document representation is transmitted to an outside agency where the current time is added to form a receipt. The agency then certifies the receipt by adding and hashing the receipt data with the current record catenate certificate which itself is a number obtained as a result of the sequential hashing of each prior receipt with the extant caternate certificate.

The certified receipt bearing the time data and the catenate certificate number is then returned to the author as evidence of the document's existence. In later proof of such existence, the certificate is authenticated by repeating the certification steps with the representation of the alleged document, the alleged time data, and the catenate certificate number appearing in the agency's records immediately prior to the certificate number in question. Only if the alleged document is identical to the original document will the original and repeat certificate numbers match.

USE - For time-stamping a digital document, for example any alphanumeric, video, audio, or pictorial data.

Dwg.1/2

US 5136647 A

The system including for example text, video, audio or pictorial data, protects the secrecy of the document text and provides a tamper proof time seal establishing an author's claim to the temporal existence of the document. The author reduces the document to a number by means of a one-way hash function, fixing a unique representation of the document text. The number is then transmitted to an outside agency where the current time is added to form a receipt which is certified by the agency using a public key signature procedure before being returned to the author as evidence of the document's existence. In later proof of such existence, the certificate is authenticated by means of the agency's public key to reveal the receipt which comprises the hash of

the alleged document along with the time seal that only the agency could have signed into the certificate.

The alleged document is then hashed with the same one-way function and the original and newly generated hash numbers are compared. A match establishes the identity of the alleged document as the time shaped original. In order to prevent collusion in the assignment of a time stamp by the agency and thus fortify the credibility of the system.

USE - For time stamping a digital document.

Dwg.1/3

数値文書にタイムスタンプを確実に押す方法　　特許第３２７８７２１号

(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許番号
特許第3278721号
(P3278721)

(45)発行日　平成14年４月30日(2002.4.30)　(24)登録日　平成14年２月22日(2002.2.22)

(51)Int.Cl.'		識別記号	FI		
G09C	1/00	640	G09C	1/00	640Z
H04L	9/32		H04L	9/00	675D

請求項の数５(全 14 頁)

(21)出願番号　特願平3－516026

(86)(22)出願日　平成３年７月30日(1991.7.30)

(65)公表番号　特表平6－501571
(43)公表日　平成６年２月17日(1994.2.17)
(86)国際出願番号　ＰＣＴ／ＵＳ９１／０５３８６
(87)国際公開番号　ＷＯ９２／０３０００
(87)国際公開日　平成４年２月20日(1992.2.20)
審査請求日　平成５年５月17日(1993.5.17)
(31)優先権主張番号　５６１，８８８
(32)優先日　平成２年８月２日(1990.8.2)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　６６６，８９６
(32)優先日　平成３年３月８日(1991.3.8)
(33)優先権主張国　米国（ＵＳ）

前置審査

(73)特許権者　591231502
テルコーディア　テクノロジーズ、インコーポレーテッド
ＢＥＬＬ　ＣＯＭＭＵＮＩＣＡＴＩＯＮＳ　ＲＥＳＥＡＲＣＨ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、ニュージャージー州、モリスタウン、サウス　ストリート　445
(72)発明者　ハバー、スチュアート、アラン
アメリカ合衆国、10003　ニューヨーク州、ニューヨーク、アーピン　プレイス　22、アパートメント　２シー
(74)代理人　100086667
弁理士　小林　孝次

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】　数値文書にタイムスタンプを確実に押す方法

(57)【特許請求の範囲】

【請求項１】数値文書の数値表現を著者側装置から外部機関装置へ送信することを含みし、上記外部機関側装置が、その受信時の時刻数値表現とこの数値文書の数値表現の少なくとも一部分とを含む受理書データを作成する、数値文書にタイムスタンプを確実に押す方法において、

受理書データが、さらに、外部機関側装置が既に受理している少なくとも一つの他の数値文書の受信時の時刻数値表現と当該少なくとも一つの他の数値文書の数値表現とを含み、

前記受領書データが含む前記少なくとも一つの他の数値文書の数値表現は、前記少なくとも１つの他の数値文書のコンテンツの少なくとも一部から導出されたものであることを特徴とする数値文書にタイムスタンプを確実に押す方法。

【請求項２】ａ）前記受理書データの数値表現を、既に鎖状につながれている証明値の表現に、さらに鎖状につないで複合表現を作り、

ｂ）前記受理書データの数値表現と前記既に鎖状につながれている証明値の表現とからなる前記複合表現に決定関数法を適用して新たな鎖状につながれた証明値を生成することをさらに含むことを特徴とする請求項１記載の方法。

【請求項３】前記外部機関側装置が、これ迄にタイムスタンプ処理した前記数値署名法により暗号化したデータを鎖状につないだ証明値の記録を維持していることを特徴とする請求項２記載の方法。

【請求項４】前記既に鎖状につながれている証明値の表現が、直前の記録済みのタイムスタンプ処理の鎖状につ

2003 11 12 16:47

ながれた証明値の少なくとも一部分を含むことを特徴とする請求項２記載の方法。

【請求項５】前記決定関数法は一方向性ハッシング法であることを特徴とする請求項４記載の方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】　文書が書かれた日付を立証し、問題の文書の内容が日付の押された原文書の内容と実際に同じであることを証明することが多くの場合に必要です。例えば、知的財産に関しては、ある人が発明の内容を最初に記録した日付を実証することは屡々決定的です。発明の考えをタイムスタンプする普通のやり方は、研究室の記録帳に自分の仕事を毎日書込むことです。消せないように日付を書いて署名した記載が記録帳の各ページに次々と書込まれ、続き番号を打たれて縫込まれたページは記録を判らないように改変することを困難にします。記録の正当性は、一般に利害関係のない第三者によって定期的に検閲され証人として署名されることによって、更に高められます。何時考えたかということが後で証明されなければいけなくなった時、記録帳の物理的な内容と定められた記録の手順の両方が、少なくとも記録帳の証人の日付の時には考えが存在していたという事実を実証する効果的な証拠となります。

【０００２】

【従来の技術】　読むことのできるテキストの数値的な表示だけでなく、ビデオやオーディオや絵のデータをも含む、電子文書が段々と広く使われるようになって来て、このような文書の日付を確立する「記録帳」の概念の実行可能性が脅かされています。電子数値文書は極めて容易に改訂され、このような改訂は後に証拠を残さないので、ある文書が作られた日付を本当にその文書が示しているのか、又元来のメッセージを今でも本当に表しているのかについては、信頼でき証拠は限られています。同じ理由で、実証する署名の信頼性についても重大な疑いが起きて来ます。数値文書の内密の改訂を許さない効果的な手順がないと、システムの信頼性が基本的に欠けていることは電子文書の有効性がもっと広く採用されることを妨げます。

【０００３】

現在でも、電子文書の送信を確証する若干の手順があります。しかし、実際にはこのような手順は両方向の通信に限られます。即ち、このような通信では、送信者は送信される文書の元の内容と送信者とを受信者に立証しようと本質的に望みます。例えば、「秘密の鍵」を使う暗号法は長い間、限られた数の、お互いに知合っていて暗号を解く鍵を知っている個人の間で、メッセージの送信に使われてきました。メッセージを暗号にすることは不正変更を防ぎ、秘密の鍵を使うと送信されたメッセージの「平文」が得られると言う事実が、メッセージは決まったグループの一員が送信したものである証拠となります。しかし、メッセージを書いた時刻は間接的に、受信者が受取った時刻より後ではないと、証明されるに過ぎません。それで、この方法は無限界世界で後になって役に立つタイムスタンプの証拠を提供しません。

【０００４】

もっと広く適用される実証通信法、即ち「公開の鍵」を使う暗号法が、ディッフィーとヘルマン（「暗号法の新しい方向」、IEEE情報理論雑誌、第IT－22巻、昭和51年11月、644－654ページ）によって既述され、その後リベスト等によって、昭和58年９月20日付のアメリカ合衆国特許４、405、829号で実行されました。この方法は利用者の世界を、公表された名簿以外ではお互いに未知の、実質上無限定数のシステム加入者に拡大しましたが、実証できる通信は依然として双方向のものに限られていました。送信者の秘密の鍵で暗号化されたメッセージを公開の鍵で解読する公開の鍵「署名」は、無限界世界のどのメンバーにもメッセージの送信者が誰であるかについて決定的な証拠を提供するものですが、このメッセージの受信者しか、メッセージは少なくとも受取った時刻以前に存在していたことを知らないわけですから、この限界は今でもあるわけです。しかし、このような受信はメッセージが発生した時刻そのものの証拠を全世界に提供はしません。受取ったメッセージに関する受信者の証言はメッセージの内容とその存在の時刻についての証拠を提供するのですが、このような証拠は電子数値文書の内容が、送信者または証人によって簡単に改変され得るという基本的な問題を抱えてもいるのです。

【０００５】

従って、総ての文書が簡単に改変できる数値形式で書かれる世界になるという予想は、このような文書の信頼性を確立する既存の手順を本質的に危うくします。数値文書の内容と時刻を確定し、少なくとも有形文書の場合に現在認められている程度に、内容と時刻に関して直接的な証拠を提供することができるような実証のシステムが現在明白に顕著に必要とされています。

【０００６】

【発明の概要】　まずこの発明が用いるタイムスタンプ手法について説明します。この手法では、数値文書をタイムスタンプする方法において信頼できるシステムを作り、現在の記録確認の本質的な特徴の二つと同等のものを提供します。第一に、文書の内容（コンテンツ）とその文書の発生時刻の刻印（タイムスタンプ）は、文書の数値データに消去不能に組込まれ、これによって出来たタイムスタンプされたデータのいかなる部分も、万一改変された場合にもその改変が明白とならない仕方で改変することは不可能であります。このように、文書の内容（コンテンツ）はタイムスタンプの瞬間に確定されます。第二に、数値文書がスタンプされた時刻は、虚偽の時刻の記載を組込むことを防ぐ、数値的に「証人として」署名する手順で確認されます。この方法とは基本的

にタイムスタンプ段階のコントロールを著者（メッセージ作成者）とは無関係な機関へと移し、真の時刻以外のスタンプをするようその機関に影響を及ぼす能力を著者から取上げます。

【０００７】

この発明が用いる上述タイムスタンプ手法は、文書の著者が通信網の中に沢山散らばって存在することを前提としています。このような著者は個人、会社、会社内の部門等で、夫々が識別番号等で特定できる。著者世界の一員です。この手法の具体例では、この著者世界はタイムスタンプ機構（タス機関）［time－stamping agency］の依頼人で構成されます。もう一つの具体例では、散らばった著者の夫々がこの世界の他のメンバーの為にタイムスタンプのサービスを行う機関となるものとなっています。

【０００８】

この発明が用いる上述タイムスタンプ手法においては、図１に示されるように、著者が広く文字、数字、音声、画面の表示を包含する数値文書を作成し、この文書を、好ましくは圧縮した形で、タス機関へ送信します。タス機関は受理した時刻を表す数値データを加えて文書にタイムスタンプし、この文書にそのタス機関の著名を入れて暗号化し、こうしてできた文書、それは今や原文書の作成時刻証明書であるが、を著者に返信し、著者はこのような作成時刻を証明することが必要になる時の為に保管します。本発明では、上述タイムスタンプ手法を用いた上で、つぎのような手順を行います。すなわち、現在時刻を特定する数値データを文書の内容（コンテンツ）に付加して文書にタイムスタンプを行って受信書を作成し、この受信書を、現時点で暗号連鎖されている、先行するタイムスタンプ受信書に連結し、さらに、この連結した複合文書から、決定関数、例えば下記に詳述するような決定関数を用いて、新たな連鎖を生成します。こうしてできた連鎖値を時刻その他の認識データと一緒にして証明書を作ります。

【０００９】

タス機関への送信中に秘密文書情報が盗聴されるのを防ぐため、また全文書の送信に要する数値帯域幅を減らすため、著者は場合によっては数値文書列を決定関数を使って数値サイズを大幅に圧縮して独自の値に変換することもします。決定関数としては、例えば専門分野で「一方向性ハッシ関数」として知られる多数のアルゴリズムのどれでも使えます。ハッシ関数のこのような応用は、例えばDamgardによって文書署名法における安全性向上策として述べられています（「衝突のないハッシ関数と公開の鍵を使う署名法」、Advances in Cryptology－－Eurocrypto ′87,Springer－Verlag,LNCS、1988、第304巻、203～217ページ）。しかし、この発明では、ハッシング法に典型的な「一方向」性がもう一つの目的を叶えてくれます。すなわち、タス機関がタイムスタンプを押したり、文書を連鎖証明書に組込んだ後では、文書は密かに改変できなくなるという保証です。

【００１０】

ハッシ関数がこの保証を提供します。というのは、著者の作成した文書もしくは複合連鎖受理書のような文書がハッシされる時、その文書を復元することが実際に不可能な元の内容に代る「指紋」を作ってしまうからです。それゆえに、タイムスタンプされた文書は著者の敵によって改変されることは不可能です。著者もまた発行されたタイムスタンプ証明書を改訂することはできません。なぜならば、原文書内容を変更することは、たとえ一語または数値データの一ビットでも、違った文書にしてしまい全く違った指紋値のものにハッシしてしまうからです。文書内容に代るハッシ値から文書を復元することはできませんが、それにもかかわらず、原文書とされているものはこのタイムスタンプ手順で証明されます。というのは指紋化された原文書の真のコピーを包含する受理書は、元のハッシング法を使えば著者の証明書に書かれた元の数字または同じ連鎖値に何時でもハッシすることができるからです。

【００１１】

この手順では現在あるどんな決定関数でも使えますが、たとえば、リベスト（「MD4」メッセージ・ダイジェスト・アルゴリズム」、Advances in Cryptology－－Crypto ′90,Springer－Verlag,LNCS、近刊予定）が述べているような一方向性ハッシ関数を引用してここに組入れて置きます。この発明の実用においては、かようなハッシング操作は場合によっては著者によって送信中の防護という著しい利点のためになされます。文書が暗号文でない形で受理された場合にはタス機関がハッシングしてもよいのです。文書の内容と組込んだ時刻のデータが改変されないように確定できるとしても、さらにこのシステムの信頼性を増すためには、無限界世界のメンバーに対して、受理書は、実は著者ではなくタス機関によって作られ、示された時刻は正しいもので、例えば著者と共謀してタス機関が偽作したようなものではないということを証明するステップがなお必要です。

【００１２】

第一の問題に対しては、タス機関が前述の公開の鍵の方法のような、実証できる署名法を用いて、著者へ送信する前にタイムスタンプを押したことを証明すればよいのです。事後的に署名を確認するには、例えば、タス機関の公開の鍵で解読するなどすれば著者と無限界世界に対して、証明書はタス機関が作ったものであることを証明することになります。しかしながら、タイムスタンプ自身の真実性の証明は、以下に述べるこの発明の構成に係るのです。

【００１３】

本発明では、タス機関は、新しく受理したものを一つ一つその時までの連鎖に付け加え、この複合表示に決定

関数を適用し、即ちハッシングを行って新たに鎖をつなげ、順次にタイムスタンプした処理の記録を維持します。この連鎖はハッシング工程で作られる値で、これが著者に与えられる受理書または証明書に記されて、そこに示されるタイムスタンプを証明するのに役立ちます。後で証明書の確認をするには、著者の時刻受理書とタス機関の記録にあるその直前の連鎖の値の組合わせに再度ハッシして行います。その結果著者の証明書に記載されている連鎖値が出れば、著者と無限界世界に対してその証明書はタス機関で作られたものであることを証明することになります。この結果はまたタイムスタンプの真実性をも証明するものです。というのは元の受理書に記載の総ての元の要素を使わなければ、ハッシ関数によって元の証明書に記載の連鎖値を作ることはできないからです。

【００１４】

図２は本発明の１実施の態様で、著者の世界からタス機関の装置へと比較的連続した文書の流れが示されています。タス機関装置は処理される夫れ夫れの文書Dkに対して、たとえば、連続する受理番号rk、著者Akの識別番号IDk、その他、文書のハッシHk、受信時の時刻tkなどを含むタイムスタンプ受理書を作成します。タス機関はこの他に、直前に処理した著者Ak－１の文書Dk－１の受理データも含め、これによって文書Dkのタイムスタンプは独自に（無関係に）確立された前の受理時刻tk－１によって「過去」方向を制限してしまいます。同様に、次に受理する文書Dk＋１の受理データも、文書Dkのタイムスタンプを「将来」方向に制限するために、含めます。複合受理書は今や３つ、あるいは希望によってはそれ以上の、連続したタイムスタンプ受理書の時刻のデータを含み、あるいはそれらの識別部分を含み、タス機関の暗号署名で証明されて、著者Akに送信されます。同様にして、DkとDk＋２の識別表示を含む証明書が著者Ak＋１に送信されます。このようにして、タス機関によって出されたタイムスタンプ証明書の夫々は連続した時間の中で確定され、配付された多数の関連した証明書を照合すれば順番の違いが直ちに判るので、タス機関はどれも偽って発行することはできません。時の流れに沿った文書のこのような順次確定は非常に効果的なので、タス機関の著名は実際には不必要かもしれません。

【００１５】

図３に書かれているように、この発明が前提とする手法では、たとえばタイムスタンププロセスを利用する多数の著者といった広い世界にタイムスタンプする仕事を無作為に配付します。タス機関を管理の目的に使ってもよく、あるいは依頼する著者が直接選択したタイムスタンプする著者兼機関と連絡してもよいわけです。いづれにしても、著者とタス機関の共謀でタイムスタンプされたのではないという保証は上記のように必要で、これは少なくとも一部の者は変造を欲する著者に買収されないか、そのような著者に暴露の脅威をもたらすという合理的な前提と、特定の文書をタイムスタンプする機関はこの世界から全く無作為に選ばれるとい事実の両方で満たされます。著者が著者自身の選択で共謀しそうな機関を選ぶことが出来ないことは、意図的な時刻の偽造の可能性を事実上除きます。

【００１６】

この所定数の機関として機能する個人ベースのメンバーを選ぶのは、インバグリアッツォ、レビンとルビー（「一方向性関数による疑似無作為創生」、第21回STOC議事録、12－24ページ、ACM、1989）によって論じられた型の疑似無作為創生機によって行います。これに対する最初の種はタイムスタンプされる文書の、ハッシのような、決定関数であります。文書に入力される種としてハッシその他の決定関数が与えられると、疑似無作為創生機は一群の機関の識別番号を出力します。この機関の選択は実際上予測できず無作為です。

【００１７】

機関が選ばれると、タイムスタンプは前述のように行われますが、夫々の機関は個々に受理時刻データを受理した文書に付け加え、その結果できたタイムスタンプされた受理書を機関固有の証明が可能な暗号署名で証明し、証明書を著者に返信します。この返信は申請した著者に直接の場合もあり、管理するタス機関を経由する場合もあり、後者の場合にはタス機関が更に証明を付け加えることもあります。署名と公表された著者の識別番号表とを組合せたものは、疑似無作為創生機で選択された機関を実際に利用したということの証明になります。この分散された機関を使う実施例は受理書を連鎖する方法に比べて、タイムスタンプ証明書がより早く発行され、また文書のある著者による事後的な証明が他の著者たちの証明書が入手できるかどうかに余り依存しなくてもよいという利点があります。

【００１８】

図４に示される別の実施例では、タス機関が作るタイムスタンプ受理書に、たとえば受理処理続き番号rk、著者の特定、たとえば識別番号IDk等、文書の数値表示、たとえばハッシHk、とその時刻tkを含めます。この後タス機関は受理書のこれらのデータ（またはその代表的な任意の部分）を、その直前に処理した、著者Ak－１の文書Dk－１の証明が記載されている連鎖値Ck－１に包含し、これによって文書Dkのタイムスタンプを、独自（無関係）に確立された前の受理時刻tk－１で限定します。

この複合データの数列（rK,IDK,Hk,tk,ck－１）はその後ハッシされて新しい連鎖値cKとなり、これが処理番号rKとともにタス機関の記録に入れられ、またタイムスタンプ受理書データとともに証明書記載連鎖値としてAKに送信されます。同様にして、ckと書類Dk＋１の受理書のタイムスタンプ要素をハッシして得られる証明書値が著者Ak＋１に送信されます。このようにして、タス機関

が出したタイムスタンプを押した連鎖証明書の夫々は連続した時の中に確定されるので、タス機関は偽って作ることは出来ません。何故ならば、前の証明書とハッシして証明書記載連鎖値を再生しようとすれば矛盾を示すからです。

【００１９】

図５に示されるような、この発明のより一般的な適用においては、ある文書の、例えばハッシのような表現はその直前の文書の連鎖値に単純に連鎖され、この複合体の決定関数による表現、たとえばやはりハッシ、が次に作られて、上記のようなある文書の連鎖値の記録として保持されます。この増大して行くシリーズの以後の夫々の文書は同様に処理されて記録を拡張し、この記録自身がこのシリーズの中で、もっと広く見れば連続した時の中で、このような文書の夫々が占める位置の信頼できる証明となります。本発明のこの実施例は、たとえばある組織がその業務上の数値文書や記録の順番や連続性を直ぐに証明できる信頼性の高い方法を提供します。

【００２０】

本発明の別の実施例では、著者の組織内で、これは活動の程度によりますが、たとえば一日とかそれ以上の一定期間に作られた、好ましくはハッシその他の表現形式の文書の集積をハッシして、タイムスタンプと証明に好都合な単一文書とします。また、疑似無作為創生機の最初の種は、その文書によるだけでなく、時刻の関数や前に受理書が出された文書にもよるかもしれません。別の方法では、一つの組織のなかの指名された一人の人が、常駐する「外部の」機関として、この手順を使ってその組織の文書の連鎖証明書の記録を維持し、定期的にその時々の連鎖証明書をタス機関に送信します。このようにして、ある組織の業務上の記録の順番が、組織の中でも、また外部的にはタス機関を通じて、確立されます。

【００２１】

また、手順実施例の実行は、原文書表示の受信・ハッシング・連鎖、タイムスタンプ押印、証明書記載連鎖値の計算と記録、受理証明書の発行という諸段階を直接行う、単一の電算機のプログラムで直ちに自動化されます。

【００２２】

【課題を解決するための手段】　前述の課題を解決するため、本発明に係る数値文書にタイムスタンプを確実に押す方法は、次のような手段を採用する。

【００２３】

即ち、請求項１では、数値文書の数値表現を著者側装置から外部機関装置へ送信することを含みし、上記外部機関側装置が、その受信時の時刻数値表現とこの数値文書の数値表現の少なくとも一部分とを含む受理書データを作成する、数値文書にタイムスタンプを確実に押す方法において、

受理書データが、さらに、外部機関側装置が既に受理している少なくとも一つの他の数値文書の受信時の時刻数値表現と当該少なくとも一つの他の数値文書の数値表現とを含み、

前記受領書データが含む前記少なくとも一つの他の数値文書の数値表現は、該少なくとも１つの他の数値文書のコンテンツの少なくとも一部から導出されたもので、

前記数値文書に決定関数法を適用して得られる数値表現の少なくとも一部分を種とする擬似無作為創生機により、一群の外部機関側装置のうちの１台を外部機関側装置として無作為に選ぶことを特徴とする。

【００２４】

また、請求項２では、請求項１の方法において、前記数値文書に一方向性ハッシング法を適用して、前記擬似無作為創生機による疑似無作為創生の種を得ることを特徴とする。

【００２５】

また、請求項３では、請求項１の方法において、前記擬似無作為創生機による擬似無作為創生によって少なくとも１台の付加的外部機関装置を選び、この付加的外部機関装置によって前記と同様に受理書データを作成することを特徴とする。

【００２６】

また、請求項４では、請求項３の方法において、前記擬似無作為創生機による擬似無作為創生によって選ばれた少なくとも１台の付加的外部機関側装置が前記と同様に受理書データを作成するものであって、夫々の付加的外部機関側装置選択のための入力が、以前に創生され出力された数値表現に前記一方向性ハッシング法を適用して得られ出力された数値表現の少なくとも一部分であることを特徴とする。

【００２７】

【発明の実施の形態】以下、本発明に係る数値文書にタイムスタンプを確実に押す方法の実施の形態を図１～図５に基づいて説明します。

【００２８】

図１は本発明に係る数値文書にタイムスタンプを確実に押す方法の基本的手順の流れ図です。

【００２９】

本発明の実施例を適用した以下の諸例で、手順を更に説明します。説明の便宜上、選ばれた決定関数は上記のリベストによって既述されたmd4ハッシング法で、また証明できる署名法はディフィーとヘルマンによって示唆されリベスト等によってアメリカ合衆国特許4,405,829号で実行された公開の鍵の方法です。タス機関が実際に選ぶ関数は色々な手に入る算法の中のどれでも良いのです。どのような算法が用いられても、何をどの機関使ったかという記録は、受理証明書を後で確認するために維持されなければなりません。更に、手順の説明を簡単にするためと以下に述べるそれ以外の理由の為に、数字の代表的な部分だけを用います。

【００３０】

図２に示される本発明の受理書連鎖の実施例を最初に考えましょう。この手順はどの様な長さの文書にも使えますが、以下の適切な引用は、ある著者が段階21で書いてタイムスタンプを希望する文書Dkを充分に代表するものです。

Time′ s glory is to calm contending kings,
To unmask falsehood, and bring truth to light,
To stamp the seal of time in aged things,
To wake the morn, and sentinel the night,
To wrong the wronger till he render right;
The Rape of Lucrece

【００３１】

破線で囲まれた任意段階22で、この文書はmd4算法によって標準の128ビットフォーマットの数HKにハッシされますが、このHkは16進法ではef6dfdcd833f3a43d4515a9fb5ce3915となります。1000人からなる著者世界の中でシステム識別番号IDKが172である著者AKがこの識別番号を付けた文書を段階23でメッセージ（ID K,H K）：172,ef6dfdcd833f3a43d4515a9fb5ce3915としてシステムのタス機関に、この文書をタイムスタンプして欲しいと要請して、送信します。

【００３２】

タス機関は、段階25で、たとえば132という受理書続き番号rKと、その時の時刻tKという記載を付け加えて、文書DKの受理書を発行します。この時刻の記載は、著者Akができたタイムスタンプ証明書を容易に読めるようにするために、電算機時計の時刻の標準32ビット表示と文章による供述を、たとえば1990年３月10日グリニジ平均時16:37:41のように含めることもできます。そうすると受理書は数列（ｒk,tk,IDk,Hk）を包含することになります。

【００３３】

この点で、数のサイズを前述の表示セグメントに減らすということを更に考えることが妥当であります。リベスト等によってアメリカ合衆国特許4,405,829号で既述されたように、この例で使われる暗号公開鍵法（この分野では一般に「RSA」署名法として知られています）では、長いメッセージを、一つ一つが暗号化鍵数要素ｎを越えない数で表わしたブロックに分割することが必要です。これらのブロック各々はこの後RSA法で署名され、送信された後ふたたび組み立てられます。それゆえに、RSA法で証明する最終の受理書数列が単一のブロックであることを維持しながら、この例で妥当な大きさの数ｎを使えるためには、受理書数列の夫々の要素は代表的な８ビットに減らされますが、長すぎる数列の場合には普通は最後の８ビットとなり、このビットは16進法では２つのヘクサデシマルの文字列となります。それで、たとえば、128ビットの文書ハッシHkは最後の８ビット、すなわち0001　0101で表され、これは16進法では15と書かれます。同様にして、IDkの172は1010　1100で、16進法ではacとなります。実際の計算を行わないで、時刻表示ｔkは51と表示されると仮定しましょう。受理番号132は84と表示されます。この点で受理書の数列（ｒk,tk,IDk,Hk）は8451ac15となりました。

【００３４】

ここで、直前の文書Dk－１はタス機関によって1990年３月10日16:32:30に（ｔk－１の表示は64）に申請201,d2d67232a61d616f7b87dc146c57574として処理されたと仮定しましょう。段階27でタス機関はこれらのデータをDkに対する受理書数列に加えて、16進法の表示、8451ac1564c974、を作ります。この受理書Rkは今やDkに対する時刻と、それ以前には著者AkがDkが存在したと主張できない時刻ｔk－１を確定するデータを含みます。Akに対するこの限定は、前の著者AK－１が時刻証明書ｃk－１を保持し、それがｔk－１は著者Ak－２の証明書にあるリンクされた時刻のデータｔk－２の以後であると確定し、というように、証明が必要なだけ続くからです。

【００３５】

タス機関が文書Dkの受理書を実際に発行したことを確立するために、段階28でタス機関は公開鍵暗号署名法で署名をし、段階29でこの受理書は著者Akに送信されて受理証明書または証明書ｃkとなります。上のようにして得られたデータを使い、またタス機関は十進法でRSA署名鍵セット

＜n,e＞＝＜43200677821428109,191＞（公開）

＜n,d＞＝＜43200677821428109,29403602422449791＞（秘密）

を持つとすれば、Rk、8451ac1564c974、に対する署名付き証明書は

Rd mod n＝39894704664774392

と計算されるでしょう。著者Akがこの証明書ｃkとRkの文章のステートメントを受取った時、タス機関の公開の鍵を適用すると

c ke mod n＝Rk

となることから、Rkは実際に文書のハッシHkを表示するデータを含んでいると確証され、ｃkが正確であると直ちに確認されます。

【００３６】

この簡単な１リンクの例の手順で作られた証明書は文書Dkのデータで時間を限定されるので、著者Ak－１に対して、文書Dk－１は文書Dkの存在のかなり前に時刻を遡らせたのではないという信頼できる証拠を提供します。Akの証明書が以後に処理された文書Dk＋１からのデータを加えて拡大された時、この証明書は同様に効果的に限定され、Akが主張するタイムスタンプを立証します。同じ効果を得る別法としては、AkにAk＋１の名を教え、Akはその著者から１リンク証明書ｃk＋１が要素Hkを含むことを確認できます。この手順は変化させて、任意の数の著者のデータを含む受理証明書を発行するようにする

こともでき、追加する毎に変造がないという保証の度合いが高まります。

【００３７】

図３に示される本発明の前提技術では著者世界の中から無作為に選ばれたメンバーがタス機関（または証人）となり、すなわち「分布信託」の手順ですが、これは以下のように行われます。実際の適用ではこれらの数はそんなには限定されないのですが、この例では、世界は1000人の著者を含み、そのIDは０ないし999で、タイムスタンプの真実性を確立するのには３人の証人がいれば充分と仮定しましょう。また、この例ではタス機関のサービスを含める前記の変化が実行されています。前の例で用いられたハッシング関数、md4、がここでも、任意の段階32で、著者世界から３人の証人を疑似無作為に選択する種をまく決定文書関数の一例として用いられています。前例の時と同じく、著者は文書をタス機関へ、普通ハッシした形で、識別番号を付けた申請として送信します：

172,ef6dfdcd833f3a43d4515a9fb5ce3915

【００３８】

タス機関は、段階33で、この文書ハッシ数列を最初の証人の識別番号を作る種として用い、段階35で、選択法

ID＝［md4（種）］mod（世界の大きさ）

によって選びます。作られた種ハッシ：

26f54eae92511dbb5e06e7c2de6e0fcf

は128ビットの数を表し、そのmod1000が487で、これが最初に選ばれた証人のIDです。次の証人も同様にして選ばれ、この種のハッシ表示を第２の選択の計算に使って

882653ee04d16b1f0d604883aa27300b

を得ますが、このmod1000は571で、これが第２の証人のIDです。この計算を繰り返し、前の種のハッシを種に使って最後の証人を598として選びますが、これは2fe8768ef3532f15c40acf1341902c1e mod1000です。

【００３９】

段階37で、タス機関は最初の申請書の写しをこれら３人の証人のそれぞれに送り、段階38で、証人は各個にその時の時刻のステートメントとIDを加え、こうしてできた受理書にRSA暗号署名法で署名して証明し、段階39で証明書を直接著者にまたはタス機関を通じて送信します。後の場合には、タス機関は証明書を一つのファイルにアセンブルして著者に届けるかも知れません。証人の選択に当たって疑似無作為創生を使うことは個人的な選択を防ぐという事実のために、著者は非協力的な証人がタイムスタンプ証明の前に虚偽の時刻の記入を計画するために連絡しようと試みるのに出あうという危険を避けられます。手順の別法として、著者が直接証人に申請することが許される場合、問題の文書自身が本質的に鍵となる証人の無作為選択により、著者が文書を知人で協力的な証人に向けようとする試みを難しくします。できた一群の証明書は、前述のように署名確認をして、安心して後の証明に使えます。

【００４０】

図４の段階41のように、タイムスタンプ手順での連鎖証明書の作成は、著者Akが数値文書を準備することから始ります。前述のように、この数値文書は文字数字式テキスト、ビデオ、オーディオ、絵または確定したデータの他の形のものの数値的な形または表示であるかもしれません。この手順はどのような長さの文書に対しても用いられますが、以下の引用はタイムスタンプしたい文書Dkを充分に代表します：

...the idea in which affirmation of the world and ethics are contained side by side...the ethical acceptance of the world and of life,together with the ideals of civilization contained in this concept...truth has no special time of its own.Its hour is now－－always.

Schweitzer

【００４１】

著者が希望すれば、文書Dkは安全と送信に必要な帯域幅を減らすために、例えばmd4法で圧縮されます。破線で囲まれた任意の段階42で示されるように、文書は標準の128ビットの形の値Hkにハッシされます。これは16進法で

ee2ef3ea60df10cb621c4fb3f8dc34c7

となります。この点で指摘しておきますが、この例で用いられる16進法やその他の数値表示は本発明の実施に決定的ではありません。すなわち、与えられた手順によって選ばれたこれらの値のどの部分もまたは他の表示も同様に作用します。

【００４２】

1000人の著者世界の中で識別番号IDkが634である著者Akが、段階43でシステムのタス機関に、以下の認識メッセージ（IDk,Hk）で、文書にタイムスタンプを押すよう要請し、文書を送信します：

634,ee2ef3ea60df10cb621c4fb3f8dc34c7

段階44で、タス機関は、受理処理続き番号ｒk、例えば1328、とその時の時刻ｔkの表示を加えて文書Dkの受理書を作ります。この時刻の表示は電算機の時計の時刻の標準２進表示かも知れず、または最終的なタイムスタンプ証明書が容易に読めるように、単に文章の表示で、例えば1991年３月６日グリニジ平均時19:46:28であるかも知れません。この時、受理書は数列（ｒk,tk,IDk,Hk）を包含し、これは

1328,194628GMT06MAR91,634,ee2ef3ea60df10cb621c4fb3f8dc34c7

となります。

【００４３】

本発明によれば、この時のタス機関の記録は、例えば、その時の記録連鎖と夫々の受理を次々とハッシしてできた値の形で、以前の受理処理総ての連鎖を含みま

す。かくして、この連鎖記録は以下のようにしてできたものです。最初の処理（ｒｋ＝１）では受理書は初期値、すなわちタス機関の認識のハッシと共にハッシされて最初の連鎖値c1を作り、これが最初の処理の証明書の値として使われます。次の処理では、受理書はc1と連鎖され、それがハッシされて第２の証明書記載連鎖値c2を作り、タス機関のタイムスタンプ業務の全歴史を通じてこれが続きます。

【００４４】

現在の例の直前に文書Dk－１がタス機関によって、第1327番目の受理業務として処理されて、証明書記載連鎖値ck－１

26f54eae92516b1f0d6047c2de6e0fcf

を作ったと仮定しましょう。手順の段階45で、タス機関はこの値とDkの受理書を連鎖して

26f54eae92516b1f0d6047c2de6e0fcf,
1328,194628GMT06MAR91,634,
ee2ef3ea60df10cb621c4fb3f8dc34c7

を作ります。この複合表示が、段階46で、タス機関にハッシされて、新しい証明書記載連鎖値ｃｋとして

46f7d75f0fbea95e96fc38472aa28ca1

を作ります。

【００４５】

この後タス機関はこの値をその記録に加えて、段階47で著者Akにタイムスタンプ証明書を送信します。これには以下の証明書記載連鎖値もふくまれます：

処理番号：　1328
依頼人識別番号:634
時刻：　19:46:28グリニジ平均時
日付：　1991年３月６日
証明書数：　46f7d75f0fbea95e96fc38472aa28ca1

この手順はタス機関によって以後のタイムスタンプ要請の都度繰り返されます。Ak＋１から次の要請がハッシされた形Hk＋１の文書

201,882653ee04d511dbb5e06883aa27300b

で1991年３月６日グリニジ平均時19:57:52に受理されたとすると、複合連鎖は

46f7d75f0fbea95e96fc38472aa28ca1,
1329,195752GMT06MAR1991,201,
882653ee04d511dbb5e06883aa27300b

となり、Ak＋１に返信される証明書は

処理番号：　1329
依頼人識別番号:201
時刻：　19:57:52グリニジ平均時
日付：　1991年３月６日
証明書数：　d9bb1b11d58bb09c2763e7915fbb83ad

となります。

【００４６】

将来、著者Ak＋１が文書Dk＋１はタス機関によって1991年３月６日19:57:52に受理されたと証明しようと望むならば、タス機関の記録が調べられ、直前に処理された1328の連鎖受領書値ｃｋ：

46f7d75f0fbea95e96fc38472aa28ca1

が得られます。証明しようとする文書はタス機関に送信された時の形、即ちハッシに変換され、この値がｃｋやその他のAk＋１の証明書に記載のデータと連鎖されます。問題の文書が本物であれば、複合表示は

46f7d75f0fbea95e96fc38472aa28ca1,
1329,195752GMT06MAR1991,201,
882653ee04d511dbb5e06883aa27300b

となり、これをハッシすると正しい証明書記載連鎖値

d9bb1b11d58bb09c2763e7915fbb83ad

となって、問題の文書はDk＋１であることが証明されます。さもなければ、改訂された文書はハッシされると違った値になり、これを要素として含む複合表示をハッシしたものは、処理番号1329の証明書に記載の値と違った証明書記載連鎖値となります。

【００４７】

もしもっと証明が必要ならば、例えば文書を改変した後でｃｋ＋１も改変したのではないかというような時には、タス機関の記録から認識されるAkの証明書と提出された、即ちハッシした文書が使われて、その後の、問題となっている証明書値ｃｋ＋１を再計算します。もしその値が正しければDk＋１は証明されました。別法としては、証明書値ｃｋ＋１は、Ak＋２の証明書値と提出された文書から次の証明書記載連鎖値ｃｋ＋２を再計算して証明されます。というのは、もしｃｋ＋１がDk＋２を処理番号1330で処理した時のものと同じでなければ、後の文書を変改してｃｋ＋２と同じ値を得るようにすることは不可能だからです。

【００４８】

図５に叙述されているもっと一般的な記録連鎖の手順では、拡大するシリーズの文書が、作られる度に、組織の中でまたはタス機関で、処理されます。段階51では、決定関数法でハッシして作られるような、新しい文書の表示が得られ、段階52では、前の文書を処理して得られた現記録連鎖値と連鎖されます。段階53では、この複合表示が処理され、すなわちハッシされ、現在の文書に対する新しい連鎖値を作ります。この値は別個に記録され、証明書に含められるか、あるいは単に処理系に保持されて段階54で提示される次の文書に適用されます。以後の処理段階55、56はこの文書表示に適用され、この手順は新しい文書が来る度に繰り返されます。

図面の簡単な説明

【図１】　文書タイムスタンプの基本的手順の流れ図です。

【図２】　この手順の具体的な実施例の流れ図です。

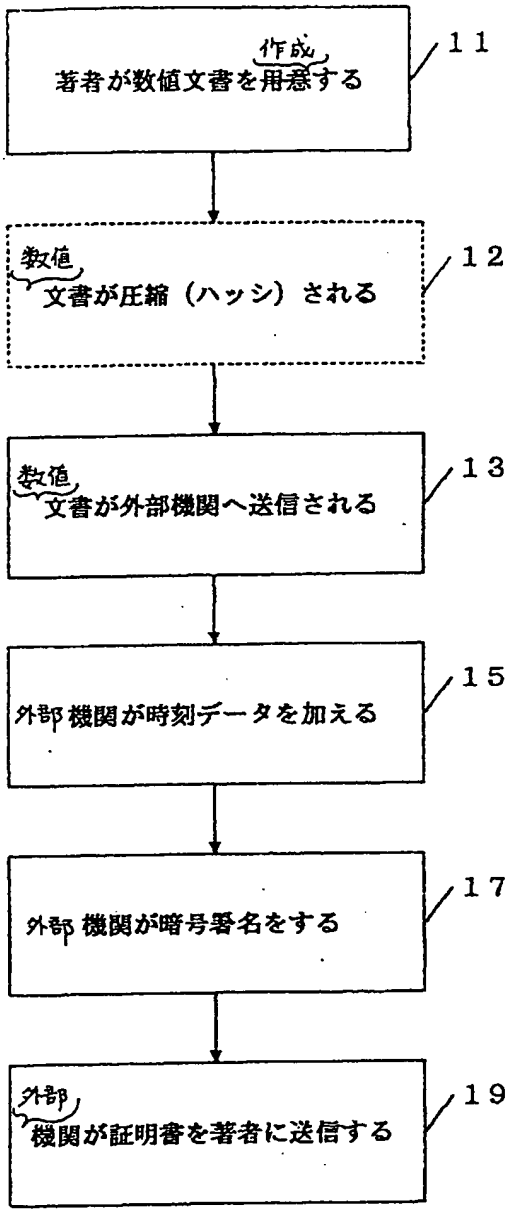
【図３】　この手順のもう一つの具体的な実施例の流れ図です。

【図４】　タイムスタンプ手順の他の実施例の流れ図で

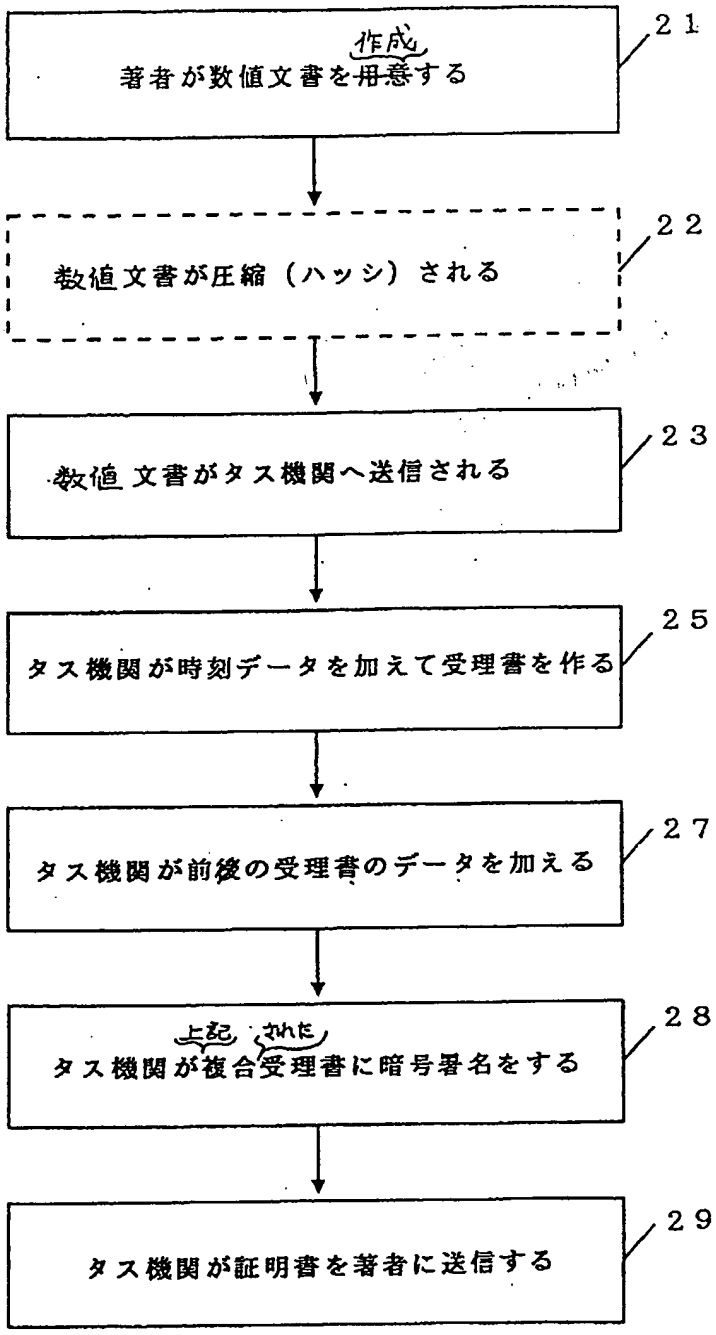
す。　　す。

【図５】　本発明による基本的な連鎖手順の流れ図で

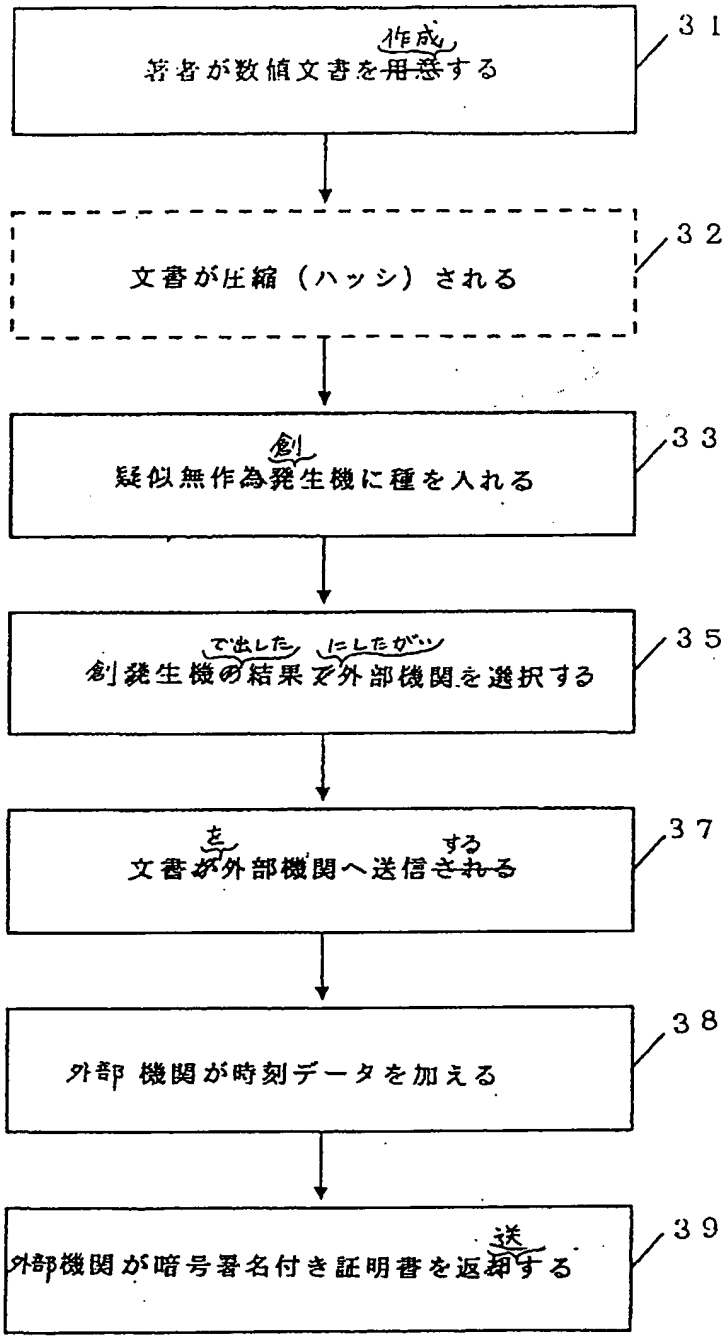
【第１図】



【第２図】

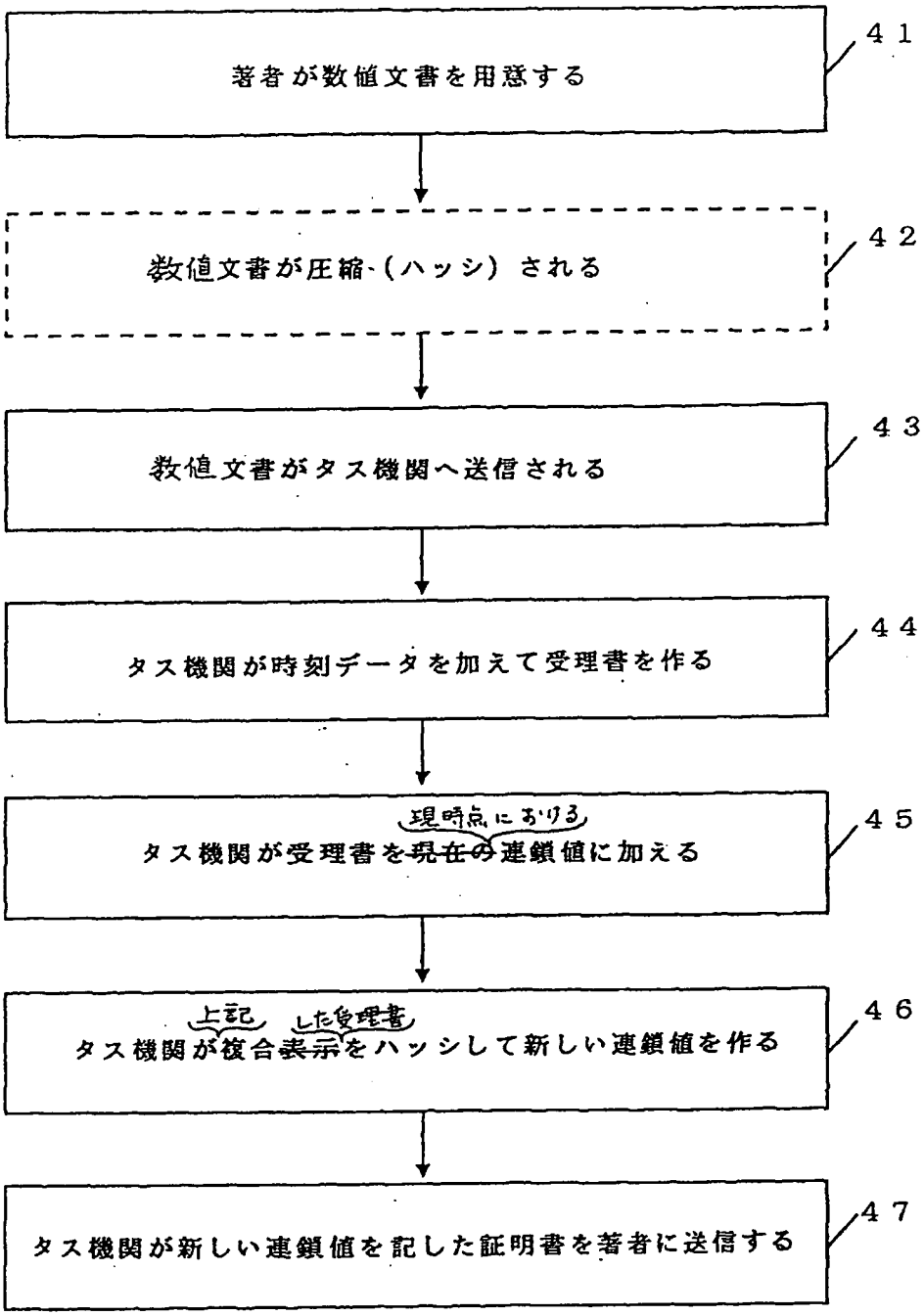

著者が数値文書を用意する
作成
21
数値文書が圧縮（ハッシ）される
22
数値文書がタス機関へ送信される
23
タス機関が時刻データを加えて受理書を作る
25
タス機関が前後の受理書のデータを加える
27
タス機関が複合受理書に暗号署名をする
上記
それに
28
タス機関が証明書を著者に送信する
29

【第３図】



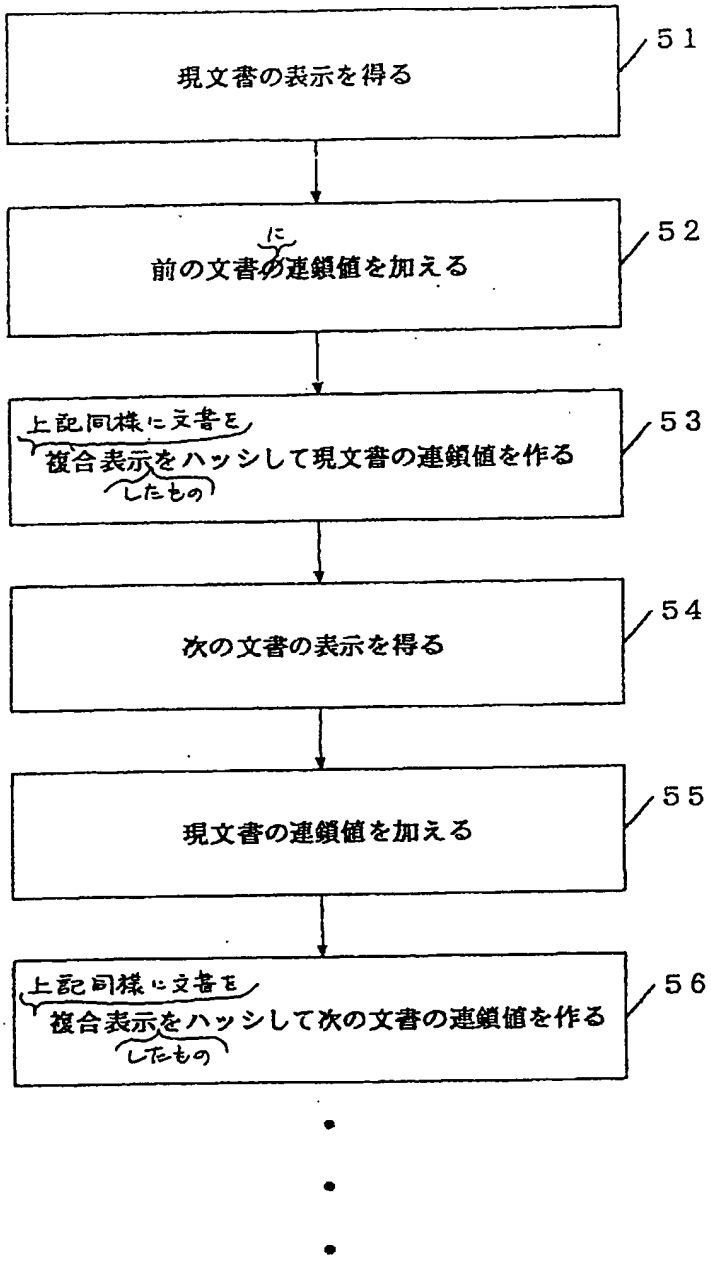
2003 11 12 16:47

【第４図】



2003 11 12 16:47

【第５図】


現文書の表示を得る
51
前の文書の連鎖値を加える
52
上記同様に文書を
複合表示をハッシュして現文書の連鎖値を作る
したもの
53
次の文書の表示を得る
54
現文書の連鎖値を加える
55
上記同様に文書を
複合表示をハッシュして次の文書の連鎖値を作る
したもの
56

フロントページの続き

(72)発明者　ストーネッタ、ウエイクフィールド、スコット、ジュニア
アメリカ合衆国、07960　ニュージャージー州、モリスタウン、ハーディングテラス　34

(56)参考文献　D. W. Davies and W. L. Price 著／上園忠弘 監訳, ネットワーク・セキュリティ, 日本, 日経マグロウヒル社, 1985年12月　5日, 1版1刷, p. 246－250
Ivan Bjerre Damgard, COLLISION FREE HASH FUNCTIONS AND PUBLIC KEY SIGNATURE SCHEMES, Leture Notes in Gomputer Science (Advances in Cryptology－EUROCRYPT' 87), 1988年　5月19日, Vol. 304, p. 203－216
W. D. Hopkins, TRANSACTION INCREMENTING MESSAGE AUTHENTICATION KEY, IBM Technical Disclosure Bulletin, 米国, 1983年　7月11日, vol. 26, no. 1, p. 199－201

(58)調査した分野(Int.Cl.[7], DB名)
G09C　1/00
H04L　9/32